Telefónica

IoT Fundamentals – Kommunikations-effizienz

Version 1.0

Einleitung

Dieses Dokument soll bei der Implementierung Ihrer IoT-Lösungen helfen, um ein Maximum an Interoperabilität, Leistung und Quality of Service zu erreichen, und hat einen rein informativen Charakter. Best-Practice-Implementierungen werden aufgezeigt, die eine effiziente und optimierte Nutzung des Mobilfunknetzes durch **IoT-Services** und die damit verbundenen Geräte gewährleisten. Ein weiteres Ziel ist die proaktive Verhinderung von Systemausfällen, die zu Überlastungen des Mobilfunknetzes oder der IoT-Service-Plattform führen.

Die in diesem Dokument beschriebenen Risiken sind nicht spezifisch für das Netz von Telefónica Germany GmbH & Co. OHG (im Weiteren **„Telefónica Germany"**), sondern gelten allgemein für alle 3GPP-Mobilfunknetze weltweit. Aus diesem Grund hat die GSMA Association die **GSMA TS.34 IoT Device Connection Efficiency Guidelines**[1] entwickelt und pflegt sie. Diese Guidelines beinhalten Hunderte von Anforderungen und Präventionsmechanismen, die von der Industrie für eine effiziente Nutzung von 3GPP-Mobilfunknetzen beigesteuert wurden. Telefónica Germany legt großen Wert darauf, seinen Kund:innen die bestmögliche Qualität des Mobilfunknetzes zu bieten, und gibt daher die wichtigsten Inhalte der GSMA TS.34 Guidelines in diesem Dokument „IoT Fundamentals" in zusammengefasster Form wieder. Zusätzliche Informationen finden Sie in den GSMA TS.34 Guidelines.
IoT-Services, die die in diesem Dokument beschriebenen Aspekte nicht berücksichtigen, können unerwünschte Folgen haben, darunter:

- verkürzte Lebensdauer der SIM-Karte aufgrund einer übermäßigen Anzahl von Lese- und Schreibzyklen;
- erhöhter Stromverbrauch des IoT-Geräts aufgrund ständiger Neustarts, was auch die Lebensdauer des Geräts verkürzen kann, und
- negative Auswirkungen auf die Leistung von IoT-Services, die möglicherweise Kommunikation verzögern oder verhindern bzw. zu einer Verschlechterung der Servicequalität oder sogar zu Ausfällen führen können.

Darüber hinaus wirkt sich eine übermäßige Nutzung oder ineffiziente Kommunikation über das Mobilfunknetz nicht nur auf die IoT-Geräte aus, die den Vorfall verursachen, sondern auch auf die IoT-Services anderer Kund:innen, die dieselbe IoT-Service-Plattform und/oder dasselbe Netz nutzen. Die Auswirkungen können z. B. Folgendes umfassen:

- regionalisierte Probleme innerhalb des Mobilfunknetzes, wie z. B. Überlastung der Zellen, und
- Kapazitäts- und Leistungsprobleme im Kernnetz des Mobilfunknetzbetreibers, die als „Signalisierungsstürme" bezeichnet werden und zu einer weiträumigen Unterbrechung des IoT-Services führen.

Zur Zielgruppe dieses Dokuments gehören Kundinnen und Kunden der Telefónica Germany, Inbound-Roaming-Kund:innen anderer (virtueller) Mobilfunknetzbetreiber, die das Telefónica Germany-Netz nutzen, IoT-Service-Provider, Hersteller von IoT-Geräten, Entwickler von IoT-Geräteanwendungen, Anbieter von IoT-Kommunikationsmodulen und Anbieter von Radio-Baseband-Chipsätzen.

Dieses Dokument „IoT Fundamentals – Connectivity Efficiency" besteht aus drei Teilen, die sich wie folgt zusammensetzen:

- Kapitel 1: Einleitung
- Kapitel 2: Begriffsbestimmungen
- Kapitel 3: Extrakt aus den GSMA TS.34 Connection Efficiency Guidelines

Bei der Durchsicht der GSMA TS.34 Guidelines in Kapitel 3 ist zu beachten, dass die GSMA Association die Einhaltung von Einträgen, die die Worte „MUSS/MÜSSEN" oder „DARF/DÜRFEN NICHT" enthalten, als verbindlich betrachtet. Im Gegenzug empfiehlt die GSMA Association die Umsetzung von Einträgen mit den Worten „SOLLTE/SOLLTEN" oder „SOLLTE/SOLLTEN NICHT".

Darüber hinaus legen die GSMA TS.34 Guidelines fest, dass für die Akteure innerhalb der IoT-Wertschöpfungskette Folgendes gilt:

- IoT-Service-Provider MÜSSEN sicherstellen, dass ihre IoT-Services und ihre IoT-Geräte-Hersteller die in den GSMA TS.34 Guidelines genannten Richtlinien erfüllen. Die IoT-Service-Provider SOLLTEN in den Lieferverträgen, die sie mit ihren IoT-Geräte-Herstellern schließen, auf die in der GSMA TS.34-Spezifikation genannten Richtlinien verweisen.
- Hersteller von IoT-Geräten MÜSSEN die in den GSMA TS.34 Guidelines genannten Richtlinien in den von ihnen hergestellten IoT-Geräten berücksichtigen. Die Hersteller von IoT-Geräten SOLLTEN in den Lieferverträgen, die sie mit ihren Partnern, den Entwicklern von IoT-Anwendungen, den Anbietern von IoT-Kommunikationsmodulen und den Anbietern von Radio-Baseband-Chipsätzen schließen, auf die GSMA TS.34-Spezifikation verweisen.
- Entwickler von IoT-Geräteanwendungen MÜSSEN sicherstellen, dass ihre IoT-Geräteanwendungen den in den GSMA TS.34 Guidelines genannten Richtlinien entsprechen.
- Hersteller von Radio-Baseband-Chipsätzen und Kommunikationsmodulen MÜSSEN sicherstellen, dass ihre Produkte den in den GSMA TS.34 Guidelines aufgeführten Richtlinien entsprechen.

[1] https://www.gsma.com/iot/gsma-iot-device-connection-efficiency-guidelines/

In diesem Dokument werden zwei „IoT Solution Layer"-Architekturen beschrieben:

- IoT-Geräteanwendungen, die die geräteseitige Service-Enablement-Logik integrieren (siehe Abbildung 1); diese Architektur – die bei weitem am meisten verbreitete – wird gemeinhin als „monolithisch" bezeichnet.
- IoT-Geräteanwendungen, bei denen die geräteseitige Service-Enablement-Logik in eine IoT-Embedded-Service-Layer-Software ausgelagert wird, wie sie beispielsweise in LwM2M-Clients oder oneM2M AE/CSEs zu finden ist (siehe Abbildung 2); diese Architektur wird gemeinhin als „mehrstufig" bezeichnet.

Abbildung 1: IoT-Lösungsschichten, monolithische IoT-Geräteanwendung

Abbildung 2: IoT-Lösungsschichten, mehrstufige IoT-Geräteanwendung

Begriffsbestimmungen

Hinweis: Die nachstehenden Definitionen beschreiben Lösungsblöcke des IoT-Stacks. Sie können auch in den Abbildungen 1 und 2 visualisiert werden (siehe Kapitel 1).

IoT-Service-Provider

Der Anbieter, der das Netz von Telefónica Germany nutzt, um einen IoT-Service bereitzustellen. Das Telefónica Germany-Netz kann das Heimat- oder Roaming-Netz der SIMs in den IoT-Geräten des IoT-Services sein.

IoT-Service

Der vom IoT-Service-Provider bereitgestellte Dienst; in der Regel handelt es sich dabei um eine vertikale M2M-Lösung, bei der IoT-Geräte wie Aktoren, Sensoren oder Gateways zur Erfassung und Übermittlung von Daten oder zur Verarbeitung vordefinierter Befehle eingesetzt werden.

IoT-Serveranwendung

Eine Anwendungssoftware, die auf einem Server läuft und mit der IoT-Service-Plattform verbunden ist, Daten austauscht und mit der IoT-Geräteanwendung über die IoT-Service-Plattform und das Telefónica Germany-Netz interagiert.

IoT-Service-Plattform

Eine Plattform, die mit der IoT-Serveranwendung verbunden ist, und die Datensitzungen mit IoT-Geräten und deren Anwendung unterhält. Das Telefónica Germany-Netz wird genutzt, um Daten zwischen der IoT-Service-Plattform und dem Kommunikationsmodul des IoT-Geräts zu übertragen. Anwendungsnachrichten können innerhalb des privaten Netzes von Telefónica Germany (einschließlich der Luftschnittstelle) über paketvermittelte, IP-basierte oder Non-IP-Datenträger übertragen werden. Darüber hinaus bietet die IoT-Service-Plattform typischerweise Service-Enablement-Funktionen für die IoT-Geräte und die IoT-Geräteanwendung und fungiert als sogenannter Geräte-Management-Server. Schließlich bietet die IoT-Service-Plattform typischerweise APIs für IoT-Serveranwendungen, um Daten auszutauschen und mit den IoT-Geräteanwendungen über die IoT-Service-Plattform zu interagieren.

Service-Enablement

Wie von den Normungsgremien definiert, kann dies Funktionen wie Geräteerkennung, Registrierung, Verwaltung (einzelner Geräte oder einer Gruppe davon), Anwendungs- und Serviceverwaltung, Kommunikationsverwaltung, Datenverwaltung, Buchung und Abrechnung sowie Abonnement und Benachrichtigung umfassen. Alle IoT-Services unterstützen die meisten dieser Befähigungsfunktionen, die zwischen den IoT-Geräten und der IoT-Service-Plattform innerhalb einer logischen Serviceschicht koordiniert werden. Sie liegt zwischen der Anwendungsschicht und der Verbindungsschicht. Auf der Seite der Geräte kann dies ein OMA-LwM2M-Client oder ein Betriebssystem sein. In der TS.34-Spezifikation wird der Service-Enablement-Layer auf dem IoT-Gerät als „IoT-Embedded-Service-Layer" bezeichnet. Auf der IoT-Service-Plattform kann ein LwM2M-Server oder ein IoT-Connector solche Operationen durchführen. Das Service-Enablement kann vom Mobilfunknetzbetreiber, dem Anbieter der IoT-Service-Plattform, dem IoT-Service-Provider oder sogar dem IoT-Geräte-Hersteller bereitgestellt werden.

IoT-Gerät

Ein Gerät, dessen Hauptfunktion darin besteht, den Fernzugriff, die Fernerkundung und/oder die Fernsteuerung von Vermögenswerten zu ermöglichen, und zwar in erster Linie über bestehende Mobilfunknetzinfrastrukturen wie das Netz von Telefónica Germany. Ein IoT-Gerät besteht aus mehreren Hardware- und Softwarekomponenten. Ein Mikrocontroller (MCU) wird in der Regel als Host für die IoT-Geräteanwendung und die Logik für das Service-Enablement verwendet. Das IoT-Kommunikationsmodul enthält einen Radio-Baseband-Chipsatz mit 3GPP-Protokollstapel, der die 3GPP-Konnektivität mit dem Mobilfunknetz aufbaut, aufrechterhält und abbaut, sowie ein Radiofrequenz-Frontend (RFFE). Eine SIM-Karte, eine Batterie, eine GNSS-Lösung, eine Benutzeroberfläche, eine Antenne, ein Sensorchip oder ein Aktor gehören zu den übrigen Komponenten, die die Architektur des IoT-Geräts ausmachen.

IoT-Geräteanwendung

Die Anwendungssoftwarekomponente, die auf der MCU des IoT-Geräts läuft, das IoT-Kommunikationsmodul über AT-Befehle steuert und mit einer IoT-Service-Plattform interagiert. Die IoT-Geräteanwendung kann zusammen mit der Logik des Service-Enablements in ein monolithisches Softwarepaket integriert werden; andernfalls kann eine mehrstufige Architektur verwendet werden, bei der die Software in eine Anwendungsschicht und eine Schicht für das Service-Enablement unterteilt ist.

Extrakt aus den GSMA TS.34 Connection Efficiency Guidelines

Kommunikation von IoT-Services (allgemein)

Die Einträge in diesem Abschnitt werden von der GSMA Association in den **„GSMA TS.34 IoT Device Connection Efficiency Guidelines“** definiert.

Vermeidung von synchronisiertem Verhalten

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS jegliches synchronisiertes Verhalten vermeiden, wenn sie die Geräteaktivierung durchführt, kommuniziert oder stattdessen ein zufälliges Muster für die Kommunikation verwendet (z. B. über einen Zeitraum von einigen Minuten bis zu mehreren Stunden oder Tagen, je nachdem, was für den Anwendungsfall des IoT-Services tolerierbar ist). Dies ist besonders kritisch im Falle einer Wiederherstellung des IoT-Services nach der Beseitigung eines netzseitigen Fehlers, da die erhöhte und konzentrierte Signalisierung und der Datenverkehr die Wiederherstellung des Netzes weiter verzögern und die Leistung des IoT-Services für alle Nutzer beeinträchtigen können.
Darüber hinaus MUSS die IoT-Service-Plattform, die mit mehreren IoT-Geräten kommuniziert, synchronisiertes Verhalten vermeiden und ein randomisiertes Muster für den Zugriff auf die IoT-Geräte innerhalb der Domäne der IoT-Service-Plattform verwenden.
Das Auslösen von Datenübertragungen, der Neustart des IoT-Geräts oder von Komponenten darin (wie dem IoT-Kommunikationsmodul oder dem Radio-Baseband-Chipsatz) oder das Senden von Geräteverwaltungsbefehlen (einschließlich, aber nicht beschränkt auf Registrierungen und Firmware-Updates) DARF NICHT synchronisiert werden. (Ref.: TS.34_4.0_REQ_003, TS.34_4.2_REQ_003 und TS.34_6.0_REQ_001)

Maximales Datenvolumen pro Monat

Die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) MUSS sicherstellen, dass die Menge der über das Telefónica Germany-Netz übertragenen Anwendungsdaten dem maximalen Datenvolumen pro einzelnes IoT-Gerät entspricht, das im Anhang dieses Dokuments angegeben ist (Hinweis: Es können tarifspezifische Ausnahmen gelten). Die im Durchschnitt zulässige maximale Nutzdatengröße pro Nachricht kann wie folgt berechnet werden: (monatliches Datenvolumen / Anzahl der Tage pro Monat) / maximale Anzahl Nachrichten pro Tag. Bitte beachten Sie, dass insbesondere schmalbandige mobile IoT-Technologien (NB-IoT und LTE-M) von nicht konformem Verhalten betroffen sind. (Ref.: TS.34_4.0_REQ_030, TS.34_4.1_REQ_005 und TS.34_4.2_REQ_030)

Überwachung des Datenverbrauchs

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS das Datenvolumen überwachen, das während eines bestimmten Zeitraums gesendet und empfangen wird. Wenn das Datenvolumen im Durchschnitt das im Anhang dieses Dokuments angegebene maximale Datenvolumen pro einzelnes IoT-Gerät überschreitet (Hinweis: Es können tarifspezifische Ausnahmen gelten), sendet die IoT-Geräteanwendung einen Bericht an die IoT-Service-Plattform und stellt weitere Anfragen für die Mobilfunkkonnektivität ein, bis die erforderliche Zeit zum Ausgleich der überschüssigen Kommunikation abgelaufen ist. Alternativ kann sie den Meldezeitraum der Anwendung anpassen, um Nachrichten weniger häufig zu senden oder die Größe der nachfolgenden Nachrichten zu reduzieren, zumindest bis das überschüssige Volumen der kommunizierten Daten ausgeglichen ist. Generell MUSS die IoT-Geräteanwendung die Daten so weit wie möglich komprimieren und eine optimierte Kodierung für die Übertragung verwenden. (Ref.: TS.34_4.0_REQ_013 und TS.34_4.2_REQ_013)

Maximale Anzahl täglicher Nachrichten

Die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) MUSS sicherstellen, dass der Berichtszeitraum der Anwendung im Durchschnitt niemals die von Telefónica Germany festgelegte tägliche Höchstzahl von Nachrichten pro einzelnes IoT-Gerät überschreitet, wie im Anhang dieses Dokuments angegeben (Hinweis: Es können tarifspezifische Ausnahmen gelten). Bitte beachten Sie, dass mobile IoT-Technologien (NB-IoT und LTE-M) besonders von nicht konformem Verhalten betroffen sind. (Ref.: TS.34_4.0_REQ_002.1, TS.34_4.0_REQ_030, TS.34_4.1_REQ_005, TS.34_4.2_REQ_002.1 und TS.34_4.2_REQ_030)

Überwachung der Anzahl der Anwendungsnachrichten

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS die Anzahl der Anwendungsnachrichten überwachen, die sie in einem bestimmten Zeitraum zu senden oder zu empfangen versucht. Wenn die Anzahl der Nachrichten im Durchschnitt die im Anhang dieses Dokuments angegebene tägliche Höchstzahl von Nachrichten pro einzelnes IoT-Gerät überschreitet (Hinweis: Es können tarifspezifische Ausnahmen gelten), sendet die IoT-Geräteanwendung einen Bericht an die IoT-Service-Plattform und stellt weitere Anfragen für die Mobilfunkkonnektivität ein, bis die erforderliche Zeit abgelaufen ist. Alternativ kann sie den Berichtszeitraum der

Anwendung anpassen, um Anwendungsnachrichten weniger häufig zu senden, zumindest bis der Überschuss ausgeglichen ist. (Ref.: TS.34_4.0_REQ_012 und TS.34_4.2_REQ_012)

„Always on"-Konnektivität bei häufiger Kommunikation

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS einen „Always on"-Verbindungsmechanismus (dauerhafte PDP/PDN-Verbindung) verwenden, wenn Daten sehr häufig gesendet werden müssen, statt jedes Mal die Netzwerkverbindungen zu aktivieren und zu deaktivieren (d.h., eine Netzwerkanbindung durchzuführen). (Ref.: TS.34_4.0_REQ_001 und TS.34_4.2_REQ_001)

Verwendung eines privaten APN

Wenn der IoT-Service mit IoT-Geräten über das Telefónica Germany-Netz kommuniziert, SOLLTE er einen privaten APN für die direkte Adressierung von IoT-Geräten mit einem eigenen, statischen IP-Adressbereich verwenden. IoT-Service-Provider sollten beachten, dass die Verwendung eines öffentlichen APN dazu führen kann, dass IoT-Geräte nach Ablauf der TCP/IP- oder UDP/IP-Sitzung auf dem Downlink nicht erreicht werden können. IoT-Geräte können jedoch jederzeit eine Uplink-Kommunikation einleiten und bei Bedarf eine neue Sitzung einrichten. (Ref.: TS.34_4.0_REQ_031 und TS.34_4.2_REQ_031)

Geräte nur aufwecken, wenn sie verbunden sind

Die IoT-Service-Plattform MUSS den Zustand des IoT-Geräts kennen und nur dann „Aufwach"-Trigger senden, wenn bekannt ist, dass das IoT-Gerät mit dem Netz verbunden ist. (Ref.: TS.34_6.0_REQ_004)

Behandlung von „Keep alive"-Nachrichten (außer NB-IoT)

Wenn die Kommunikation mit dem IoT-Gerät innerhalb des Heim- oder Roaming-Netzes auf TCP/IP basiert, ist die Verwendung von TCP-„Keep alive"-Abfragen erforderlich, um die TCP-Sitzung aktiv zu halten, wenn der Zeitraum der Kommunikation länger ist als der Timer der TCP-Sitzung. Verwendet das IoT-Gerät stattdessen das UDP/IP-Protokoll, muss es sich entweder an den kürzeren Wert des UDP-Session-Timers anpassen oder jedes Mal, wenn es über den Uplink kommunizieren will, eine neue UDP-Sitzung aufbauen.
In solchen Fällen MUSS die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) automatisch die sitzungsspezifischen Zeitgeber und/oder die Network-Address-Translation (NAT)-Timer der Mobilfunk-Firewall erkennen, z.B. den „TCP_IDLE"-Wert oder den „UDP_IDLE"-Wert. Dies wird erreicht, indem das Abfrageintervall dynamisch erhöht wird, bis eine Zeitüberschreitung im Mobilfunknetz auftritt, und dann knapp unter dem Zeitüberschreitungswert gearbeitet wird. Bitte beachten Sie, dass viele Roaming-Netze einen NAT-Time-out-Wert von weniger als 30 Minuten verwenden; TCP/IP-Session-Timer können länger sein, z.B. bis zu 2 Stunden.
Feste Abfrageintervalle SOLLTEN von der monolithischen IoT-Geräteanwendung (oder dem separaten IoT-Embedded-Service-Layer auf dem IoT-Gerät) idealerweise NICHT verwendet werden, da sich die Werte für die Abfrageintervalle je nach Belastung des Mobilfunknetzes ändern oder dynamisch anpassen können. Lässt sich dies nicht vermeiden, SOLLTE die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) die Remote- und/oder lokale Konfiguration des Intervalls dieser „Keep alive"-Nachrichten ermöglichen. (Ref.: TS.34_4.0_REQ_006, TS.34_4.0_REQ_007, TS.34_4.2_REQ_006 und TS.34_4.2_REQ_007)

Priorisierung von Anwendungsdaten

Die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) SOLLTE die Priorität (Wichtigkeit und Dringlichkeit) der Daten klassifizieren, bevor sie entscheidet, ob Nachrichten über das Netz gesendet werden sollen, um die Überlastung des Netzes zu minimieren. So kann beispielsweise unterschieden werden zwischen Daten, die eine sofortige Übertragung erfordern, und verzögerungstoleranten Daten, die aggregiert und/oder zu „verkehrsschwachen" Zeiten (z.B. in den frühen Morgenstunden) gesendet werden könnten. (Ref.: TS.34_4.0_REQ_018, TS.34_4.1_REQ_003 und TS.34_4.2_REQ_018)

Kommunikation außerhalb von Zeiten hoher Netzauslastung

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) SOLLTE so konzipiert sein, dass die Netzkommunikationsaktivität der Anwendung nicht in Zeiten hoher Netzauslastung (z.B. in den frühen Morgenstunden) konzentriert wird. Bitte beachten Sie, dass solche „Spitzenzeiten" je nach Anwendung unterschiedlich sein können. (Ref.: TS.34_4.0_REQ_016 und TS.34_4.2_REQ_016)

Lokalisierte, intensive Kommunikation

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS das Risiko geografischer Netzbelastungsprobleme minimieren, die beispielsweise durch die Auslösung von Vorgängen in einem kleinen geografischen Gebiet verursacht werden, die einen hohen Netzverkehr verursachen, z.B. Firmware-Updates, die auf einmal an alle Geräte in einer Stadt ausgeliefert werden. Darüber hinaus MUSS der IoT-Service alle geografischen Netzbelastungsprobleme tolerieren, die aufgrund externer Faktoren, die außerhalb seiner Kontrolle liegen, dennoch auftreten können. (Ref.: TS.34_4.0_REQ_017 und TS.34_4.2_REQ_017)

IoT-Service-Koordination

Wenn die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) mit mehreren IoT-Serveranwendungen kommuniziert, die dasselbe IoT-Kommunikationsmodul oder denselben Radio-Baseband-Chipsatz verwenden, SOLLTE sie die Übertragung der Nutzdaten jedes IoT-Services so koordinieren, dass das Netz effizient genutzt wird. (Ref.: TS.34_4.0_REQ_002 und TS.34_4.2_REQ_002)

Extrakt aus den GSMA TS.34 Connection Efficiency Guidelines

Kommunikation von IoT-Services (allgemein)

Authentifizierung und Verschlüsselung der Kommunikation

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) SOLLTE alle Anwendungsnachrichten Ende-zu-Ende-verschlüsselt senden und die IoT-Service-Plattform vor der Datenkommunikation authentifizieren. Ebenso SOLLTE die IoT-Service-Plattform das IoT-Gerät vor der Datenkommunikation authentifizieren. Die Stärke der verwendeten Authentifizierung ist so zu bemessen, dass sie für den IoT-Service angemessen ist.
Diese Vorkehrungen stellen sicher, dass IoT-Geräte und/oder die IoT-Service-Plattform nicht kompromittiert werden, was möglicherweise sogar zu einem DDoS-Angriff (Distributed Denial of Service) auf das Mobilfunknetz führen könnte. (Ref.: TS.34_4.0_REQ_020, TS.34_4.0_REQ_021, TS.34_4.2_REQ_020, TS.34_4.2_REQ_021 und TS.34_6.0_REQ_005)

Vermeidung von MQTT oder HTTP bei Verwendung von NB-IoT

Wenn die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) über einen NB-IoT-Träger kommuniziert, SOLLTE sie MQTT- oder HTTP-Nachrichten-/-Verwaltungsprotokolle NICHT verwenden, da deren TCP/IP-sitzungsbasierte Verbindungen nicht für NB-IoT optimiert sind. Ideal sind verbindungslose Protokolle wie CoAP oder MQTT-SN, da diese es ermöglichen, den darunterliegenden UDP/IP-Träger einzurichten und zu entfernen. Ebenso können bestehende DTLS-Sitzungen, anders als bei TLS über TCP/IP, über aufeinanderfolgende UDP/IP-Sitzungen fortgesetzt werden. (Ref.: TS.34_4.0_REQ_031 und TS.34_4.2_REQ_031)

Vermeidung von „Keep alive"-Nachrichten bei Verwendung von NB-IoT

Wenn die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) über einen NB-IoT-Träger kommuniziert, SOLLTE sie TCP- oder UDP-„Keep alive"-Nachrichten im Heim- oder Roaming-Netzwerk NICHT implementieren. Berücksichtigen Sie bitte die Auswirkungen auf die Batterielebensdauer bei wiederholter TCP/IP-, TLS-, MQTT- oder HTTP-Sitzungsaushandlung bei der Kommunikation. (Ref.: TS.34_4.0_REQ_006.1 und TS.34_4.2_REQ_006.1)

Extrakt aus den GSMA TS.34 Connection Efficiency Guidelines

Fehlerbehandlung und Wiederherstellung

Die Einträge in diesem Abschnitt werden von der GSMA Association in den **„GSMA TS.34 IoT Device Connection Efficiency Guidelines"** definiert.

Verhalten, wenn das SIM-Abonnement vorübergehend inaktiv ist

Wenn das mit einem IoT-Gerät verbundene SIM-Abonnement vorübergehend in einen inaktiven Zustand versetzt werden soll (d.h., das Abonnement soll für einen bestimmten Zeitraum deaktiviert werden), MUSS der IoT-Service-Provider zunächst über IoT-Geräteanwendungslogik sicherstellen, dass das IoT-Gerät vorübergehend deaktiviert wird, um zu verhindern, dass das Gerät versucht, sich im Netz zu registrieren, sobald die SIM deaktiviert ist. (Ref.: TS.34_6.0_REQ_002)

Verhalten bei dauerhafter Deaktivierung des SIM-Abonnements

Bevor das mit einem IoT-Gerät verbundene SIM-Abonnement in einen dauerhaft beendeten Zustand übergeht, MUSS der IoT-Service-Provider über IoT-Geräteanwendungslogik sicherstellen, dass das IoT-Gerät dauerhaft deaktiviert wird, um zu verhindern, dass das Gerät versucht, sich im Netz zu registrieren, sobald die SIM dauerhaft deaktiviert ist.
Der IoT-Service-Provider SOLLTE sorgfältig in Erwägung ziehen, IoT-Geräte, die nicht einfach gewartet werden können, dauerhaft abzuschalten, da ein manueller Eingriff (d.h. ein Serviceaufruf) erforderlich sein kann, um die IoT-Geräte wieder zu aktivieren. (Ref.: TS.34_6.0_REQ_002)

Verhalten bei niedrigem Batteriestand oder Stromausfall

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) SOLLTE bei einem unerwarteten Batterieproblem eine Benachrichtigung mit relevanten Informationen an die IoT-Service-Plattform senden. Bei einem Stromausfall können IoT-Geräte die IoT-Service-Plattform auf nicht synchrone Weise benachrichtigen, obwohl dies bei der Kommunikation über NB-IoT auf eine besondere Weise zu implementieren ist (siehe die entsprechende Richtlinie im vorherigen Abschnitt). (Ref.: TS.34_4.0_REQ_014 und TS.34_4.2_REQ_014)

Verhalten bei IoT-Geräten, die nicht auf SMS-Trigger reagieren

Wenn die IoT-Service-Plattform SMS-Trigger zum „Aufwecken" von IoT-Geräten verwendet, MUSS sie es vermeiden, mehrere SMS-Trigger zu senden, sofern innerhalb eines bestimmten Zeitraums keine Antwort eingeht. (Ref.: TS.34_6.0_REQ_003)

Verhalten bei Kommunikationsfehlern im Heimat- und Roaming-Netz

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) ist immer darauf vorbereitet, mit Situationen umzugehen, in denen Kommunikationsanfragen im Heimnetzwerk oder beim Roaming fehlschlagen:

- Sie MUSS versuchen, die Konnektivität auf höheren Verbindungsschichten wiederherzustellen (z.B. per VPN-Tunnel, SSH-Sitzungen).
- Sie MUSS feststellen, ob die Kommunikationsprobleme mit dem Server durch Kommunikationsprobleme auf höheren Verbindungsschichten (innerhalb des MQTT[-SN]-, HTTP-, CoAP-, TCP/IP- oder UDP/IP-Protokolls) verursacht werden.
- Sie MUSS versuchen, die PDN-Konnektivität oder den PDP-Kontext wiederherzustellen.
- Sie MUSS versuchen, sich wieder mit dem Mobilfunknetz zu verbinden.
- Sie MUSS ein Netzauswahlverfahren durchführen.
- Als letzte Möglichkeit MUSS sie das IoT-Kommunikationsmodul oder den Radio-Baseband-Chipsatz nach dem Zufallsprinzip zurücksetzen, was zu einem erneuten Aufbau der RRC-Verbindung führt. Wiederholungsversuche MÜSSEN exponentiell verzögert werden.
- Mechanismen höherer Verbindungsschichten MÜSSEN daraufhin versuchen, die Verbindung mit der IoT-Service-Plattform wiederherzustellen.

Die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) DARF NICHT häufig einen Neustart des IoT-Kommunikationsmoduls oder des Radio-Baseband-Chipsatzes veranlassen. Stattdessen MUSS sie Verbindungsanfragen an die IoT-Service-Plattform mit zunehmender Verzögerung wiederholen. Solche Wiederholungsmechanismen können variieren und hängen von der Bedeutung und dem Volumen der heruntergeladenen Daten ab. Mögliche Lösungen können sein:

- das einfache Zählen der Fehlversuche seit dem ersten Aufbau der Datenverbindung (oft die einfachste Lösung) oder
- die Überwachung der Anzahl der Fehlversuche innerhalb eines bestimmten Zeitraums. Wenn z. B. die Datenverbindung innerhalb einer Stunde mehr als fünfmal unterbrochen wird, können die Anfragen ausgesetzt werden. Dies kann eine zuverlässigere Technik sein, um kurzzeitige, aber regelmäßige Verbindungsprobleme zu vermeiden, z. B. wenn sich ein IoT-Gerät von einer Netzzelle zu einer anderen bewegt. Die Datenverbindung kann unterbrochen werden, wenn das IoT-Gerät zwischen den Zellen wechselt, aber wenn die Zelle eine gute Abdeckung bietet, kann die Anfrage erfolgreich bearbeitet werden.

Je nach IoT-Service SOLLTE keine Kommunikationsanforderung der IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) unbegrenzt wiederholt werden – die Anforderung wird schließlich durch Zeitüberschreitung abgebrochen. (Ref.: TS.34_4.0_REQ_011, TS.34_4.0_REQ_029, TS.34_4.1_REQ_002, TS.34_4.2_REQ_011 und TS.34_4.2_REQ_029)

Verhalten bei Verlust des GNSS-Empfangs

Wenn die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) feststellt, dass die GNSS-Abdeckung (z. B. GPS, GLONASS, BeiDou oder Galileo) verloren gegangen ist und der GNSS-Empfänger auf dem IoT-Kommunikationsmodul oder dem Radio-Baseband-Chipsatz gehostet wird, DARF sie das IoT-Gerät, das IoT-Kommunikationsmodul oder den Radio-Baseband-Chipsatz NICHT neu starten.
Stattdessen MUSS die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) den Scanvorgang wiederholen, um eine mobile GNSS-Abdeckung mit zunehmender Verzögerung zu erfassen. Wenn dies fehlschlägt, SOLLTE sie eine Diagnose durchführen und eine Fehlermeldung an die IoT-Serveranwendung senden.
Wenn der GNSS-Empfänger nicht auf dem IoT-Kommunikationsmodul oder dem Radio-Baseband-Chipsatz untergebracht ist, SOLLTE die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) die betroffene Hardwarekomponente (z. B. den GNSS-Chip) neu starten, eine Diagnose durchführen und eine Fehlermeldung an die IoT-Serveranwendung senden. (Ref.: TS.34_4.0_REQ_034, TS.34_4.0_REQ_035, TS.34_4.2_REQ_034 und TS.34_4.2_REQ_035)

Verhalten bei Verlust der LAN-Verbindung

Wenn die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) feststellt, dass die LAN-Konnektivität mit Peripheriegeräten verloren gegangen ist, und die LAN-Konnektivitätsfunktion auf dem IoT-Kommunikationsmodul oder dem Radio-Baseband-Chipsatz gehostet wird, DARF sie das IoT-Gerät, das IoT-Kommunikationsmodul oder den Radio-Baseband-Chipsatz NICHT neu starten. Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS den Scanvorgang wiederholen, um eine mobile LAN-Verbindung mit zunehmender Verzögerung zu erhalten. Wenn dies fehlschlägt, SOLLTE sie eine Diagnose durchführen und eine Fehlermeldung an die IoT-Serveranwendung senden.
Wenn die LAN-Konnektivitätsfunktion nicht auf dem IoT-Kommunikationsmodul oder dem Radio-Baseband-Chipsatz gehostet wird, SOLLTE die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) eine Diagnose durchführen, die betroffene Hardwarekomponente (z. B. den Wi-Fi-Transceiver) neu starten und eine Fehlermeldung an die IoT-Serveranwendung senden. (Ref.: TS.34_4.0_REQ_036, TS.34_4.0_REQ_037, TS.34_4.2_REQ_036 und TS.34_4.2_REQ_037)

Verhalten bei Fehlfunktion oder Auslösung von Sensoren oder Aktoren

Wenn eingebaute Sensoren oder Aktoren eine Fehlfunktion aufweisen oder ausgelöst werden, DARF die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) das IoT-Gerät, das IoT-Kommunikationsmodul oder den Radio-Baseband-Chipsatz NICHT neu starten. Sie SOLLTE eine Diagnose durchführen, die betroffene Hardwarekomponente (z. B. die Sensoren- oder Aktorenkomponente) neu starten und eine Fehlermeldung an die IoT-Serveranwendung senden. (Ref.: TS.34_4.0_REQ_038, TS.34_4.0_REQ_039, TS.34_4.2_REQ_038 und TS.34_4.2_REQ_039)

Verhalten, wenn der Gerätespeicher voll ist

Wenn der Speicher des IoT-Geräts voll ist, z. B. aufgrund der Menge der gesammelten Daten oder eines unerwünschten Speicherlecks, DARF die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) das IoT-Gerät, das IoT-Kommunikationsmodul oder den Radio-Baseband-Chipsatz NICHT neu starten. Sie SOLLTE eine Diagnose durchführen, die betroffene Hardwarekomponente (z. B. den integrierten Speicher) neu starten und eine Fehlermeldung an die IoT-Serveranwendung senden. (Ref.: TS.34_4.0_REQ_032, TS.34_4.0_REQ_033, TS.34_4.2_REQ_032 und TS.34_4.2_REQ_033)

Extrakt aus den GSMA TS.34 Connection Efficiency Guidelines

Richtlinien für IoT-Geräte

Die Einträge in diesem Abschnitt werden von der GSMA Association in den **„GSMA TS.34 IoT Device Connection Efficiency Guidelines"** definiert.

Radio Policy Manager

Bei einer großen Anzahl von IoT-Geräten (z.B. mehr als 2.000 Einheiten innerhalb desselben Mobilfunknetzes) SOLLTE der IoT-Dienste-Anbieter in seinen IoT-Geräten ein IoT-Kommunikationsmodul einsetzen, dessen Radio-Baseband-Chipsatz die Funktion „Radio Policy Manager" (RPM) unterstützt, wie in der Spezifikation GSMA TS.34, Abschnitt 8, definiert. Diese Funktion sollte für das Telefónica Germany-Netz aktiviert sein. (Ref.: TS.34_5.2_REQ_001)

Vermeidung von Mechanismen, die das Modem häufig neu starten

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) DARF einen Mechanismus NICHT implementieren, der einen häufigen Neustart des IoT-Kommunikationsmoduls oder des Radio-Baseband-Chipsatzes auslöst. (Ref.: TS.34_4.0_REQ_019 und TS.34_4.2_REQ_019)

Low Power Mode

Wenn eine IoT-Geräteanwendung keine regelmäßigen Datenübertragungen durchführen muss und eine gewisse Latenz für ihren IoT-Dienst tolerieren kann, SOLLTE die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) einen „Stromspar"-Betriebsmodus implementieren, bei dem das IoT-Gerät und sein IoT-Kommunikationsmodul oder sein Funk-Basisband-Chipsatz zwischen den Datenübertragungen tatsächlich abgeschaltet werden. Dadurch wird der Stromverbrauch des IoT-Geräts weiter gesenkt und die Netzsignalisierung minimiert. (Ref.: TS.34_4.0_REQ_020, TS.34_4.1_REQ_004 und TS.34_4.2_REQ_020)

Zurücksetzen auf Werkseinstellungen

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) SOLLTE ein Zurücksetzen auf Werkseinstellungen über eine Remote- und lokale Verbindung unterstützen. (Ref.: TS.34_4.0_REQ_024 und TS.34_4.2_REQ_024)

Nachselektion zwischen 3GPP- und Nicht-3GPP-Zugang

Wenn das IoT-Gerät mehr als eine Familie von Kommunikationszugangstechnologien unterstützt (z.B. 3GPP-Technologien und Wireless LAN), SOLLTE die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) einen Schutzmechanismus implementieren, um ein häufiges „Pingpong" zwischen diesen verschiedenen Familien von Kommunikationszugangstechnologien zu verhindern. Die Einführung einer Hysterese oder eines zufälligen Timers sind mögliche praktische Umsetzungen. (Ref.: TS.34_4.0_REQ_026, TS.34_4.0_REQ_027, TS.34_4.2_REQ_026 und TS.34_4.2_REQ_027)

Überwachung der Geschwindigkeit und Verbindungsqualität von Mobilfunknetzen

Wenn die Datengeschwindigkeit und die Latenzzeit für den IoT-Dienst von entscheidender Bedeutung sind, SOLLTE die monolithische IoT-Geräteanwendung (oder die IoT-Geräteanwendung und der darunterliegende IoT-Embedded-Service-Layer) die Geschwindigkeit des Mobilfunknetzes und die Verbindungsqualität ständig überwachen, um die entsprechende Servicequalität von der IoT-Service-Plattform anzufordern. (Ref.: TS.34_4.0_REQ_010, TS.34_4.1_REQ_001 und TS.34_4.2_REQ_010)

Anpassung an Mobilfunknetzkapazitäten, Datengeschwindigkeit und Latenzzeit

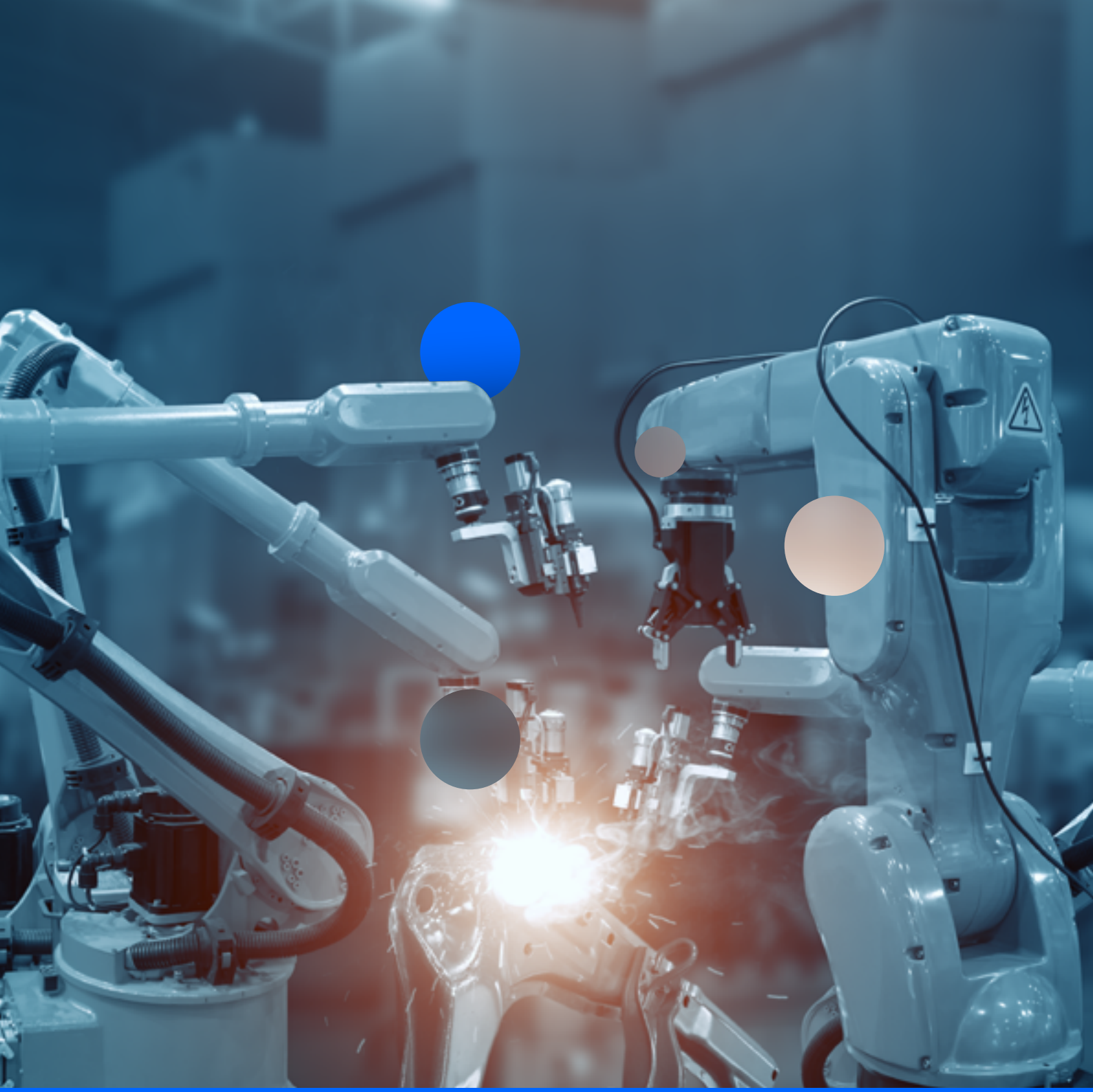
Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS in der Lage sein, sich an Änderungen bei der Leistungsfähigkeit des Mobilfunknetzes und der Dienstnutzung anzupassen. Darüber hinaus ist sie so konzipiert, dass sie mit Schwankungen des verfügbaren Durchsatzes, der Datengeschwindigkeit und der Latenz des Mobilfunknetzes umgehen kann, insbesondere beim Wechsel zwischen verschiedenen Funkzugangstechniken (d.h. NB-IoT, LTE-M, 2G, 3G, LTE oder 5G-NSA). (Ref.: TS.34_4.0_REQ_008, TS.34_4.0_REQ_009, TS.34_4.2_REQ_008 und TS.34_4.2_REQ_009)

IPv4/v6-Dual-Stack-Unterstützung

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) MUSS IPv4/v6-Dual-Stack unterstützen (PDN-Typ = IPv4/v6), damit sie ordnungsgemäß in Roaming-Mobilfunknetzen agieren kann, die entweder nur IPv4, nur IPv6 oder nur Dual-Stack unterstützen. (Ref.: TS.34_5.3_REQ_006)

Resynchronisation der Gerätezeit

Die monolithische IoT-Geräteanwendung (oder der separate IoT-Embedded-Service-Layer auf dem IoT-Gerät) SOLLTE die Resynchronisierung von Zeit über eine Remote- und eine lokale Verbindung unterstützen. (Ref.: TS.34_4.0_REQ_025 und TS.34_4.2_REQ_025)



Herausgeber
Telefónica Deutschland GmbH & Co. OHG

Georg-Brauchle-Ring 50
80992 München
iot.telefonica.de

Verantwortlich für den Inhalt
O_2 Telefónica
Digital Services – IoT, Miguel Rodriguez

Bildnachweis
Telefónica Deutschland